WHAT IS CLAIMED IS:

Sub A1

1. A mutual authentication method for use between a recording apparatus which records copied contents on a recording medium having an arithmetic processing function, and the recording medium, said method comprising the steps of:

storing in the recording medium at least first information which depends on the recording medium, and second information which is to be shared by the recording apparatus in executing mutual authentication with the recording apparatus and depends on the recording medium; and

generating by the recording apparatus authentication information used in mutual authentication with the recording medium on the basis of the first information obtained from the recording medium, and executing mutual authentication between the recording apparatus and the recording medium using the generated authentication information and the second information.

2. The method according to claim 1, further comprising the step of:

generating the authentication information by encrypting the first information using an encryption key obtained from the recording medium.

3. A mutual authentication method for use between a reproducing apparatus which reproduces copied

contents recorded on a recording medium having an arithmetic processing function, and the recording medium, said method comprising the steps of:

storing in the recording medium at least first information which depends on the recording medium, and second information which is to be shared by the reproducing apparatus in executing mutual authentication with the reproducing apparatus and depends on the recording medium; and

generating by the reproducing apparatus authentication information used in mutual authentication with the recording medium on the basis of the first information obtained from the recording medium, and executing mutual authentication between the reproducing apparatus and the recording medium using the generated authentication information and the second information.

4. The method according to claim 3, further comprising the step of:

generating the authentication information by encrypting the first information using an encryption key obtained from the recording medium.

5. A recording apparatus for recording copied contents on a recording medium while limiting the number of copied contents to be recorded on the recording medium, said apparatus comprising:

generation means for generating authentication

information, which is used in mutual authentication with the recording medium and is to be shared by the recording medium, on the basis of first information which is obtained from the recording medium and depends on the recording medium; and

mutual authentication means for executing mutual authentication with the recording medium using the authentication information generated by said generation means.

6. An apparatus according to claim 5, wherein said generation means generates the authentication information by encrypting the first information using an encryption key obtained from the recording medium.

7. A reproducing apparatus for reproducing copied contents recorded on a recording medium while limiting the number of copied contents to be recorded on the recording medium, said apparatus comprising:

generation means for generating authentication information, which is used in mutual authentication with the recording medium and is to be shared by the recording medium, on the basis of first information which is obtained from the recording medium and depends on the recording medium; and

mutual authentication means for executing mutual authentication with the recording medium using the authentication information generated by said generation means.

8. An apparatus according to claim 7, wherein said generation means generates the authentication information by encrypting the first information using an encryption key obtained from the recording medium.

9. A recording medium having an arithmetic processing function, comprising:

storage means for pre-storing first information which is unique to said recording medium, and second information which is to be shared by a recording apparatus for recording copied contents on said recording medium and a reproducing apparatus for reproducing the copied contents in executing mutual authentication among the recording medium, the recording apparatus, and the reproducing apparatus, and depends on said recording medium; and

mutual authentication means for executing mutual authentication between the recording medium and the recording apparatus, and between the recording medium and the reproducing apparatus using authentication information generated based on the first information by the recording apparatus and the reproducing apparatus, and the second information.